Nassau County
Office of the Comptroller
Field Audit Bureau

Nassau County Computer Systems' Disaster-Recovery Preparedness

<u>**HOWARD S. WEITZMAN**</u>

Comptroller

MA02-04

SEPTEMBER 4, 2002

NASSAU COUNTY
OFFICE OF THE COMPTROLLER

HOWARD S. WEITZMAN
Comptroller

Jane R. Levine
Chief Deputy Comptroller

Jacques Jiha
Deputy Comptroller
for Audits and Finance

Salim Ejaz
Director of Field Audit

Bruce G. Kubart
Assistant Director of Field Audit

Audit Staff

Janis McDermott
Field Auditor IV

Richard Wagner
Field Auditor II

Susan D. Wagner
Deputy Comptroller
for Operations

Michael Kornfeld
Communications Director

Executive Summary

Background

The September 11 terrorist attack on the World Trade Center provides a powerful reminder of the importance of effective disaster recovery preparedness for all technology-dependent institutions. While it is not possible for even the most farsighted government or organization to envision and prepare for every possible danger, we can anticipate and prepare for the adverse effects of a catastrophe, whatever its cause. A disaster to Nassau County could result from any condition that would prevent the county from performing critical business and governmental functions in an acceptable period of time. Hurricanes, tornadoes, earthquakes, floods, fires, technological failures, power outages, and large-scale acts of violence, including terrorist actions, are examples of disasters that could seriously disrupt critical computer systems.

Technology, while providing great utility to the county, at the same time renders it more vulnerable to disaster losses. Even a short-term downtime of critical computer applications can jeopardize county services. It is vital that the county create, rehearse, and regularly revise, as necessary, a comprehensive disaster-recovery plan (DRP) for worst-case scenarios.

New York State law, § 20, State and Local Natural and Man-Made Disaster Preparedness, Article 2-B, requires that local government and emergency service organizations have an essential role as the first line of defense in times of disaster. State policy requires that local chief executives take an active and personal role in the development and implementation of disaster preparedness programs and that they be vested with authority and responsibility in order to insure the success of such programs. The state's policy also indicates that state and local plans, organizational arrangements, and response capabilities shall at all times be the most effective that current circumstances and existing resources allow.

In 1999, the Government Finance Officers Association (GFOA) recommended that every government should formally establish and regularly update written policies and procedures for minimizing disruptions resulting from information or other technology failures following a disaster. At a minimum, the GFOA stated these policies and procedures should include assignment of disaster-recovery coordinators, creation and preservation of backup data, provisions for alternate processing following a disaster, detailed instructions for restoring disk files, and guidelines for the immediate aftermath of a disaster.

Scope and Methodology

The scope of this audit is to evaluate the disaster preparedness of the major computer systems throughout Nassau County that are maintained by the Division of Information Technology, the Police Department and Nassau Community College. The scope did not include review of the exposure of the hardware to physical threats or damages. During the audit, we interviewed key personnel responsible for the county's computer systems and analyzed relevant documentation. Our examination was performed during the first quarter of 2002.

The audit was conducted in accordance with generally accepted government auditing standards as promulgated by the Comptroller General of the United States. These standards require that the audit is planned and performed to obtain reasonable assurance that the information, which is audited, is free of material misstatements. An audit includes examining documents and other available evidence that would substantiate the accuracy of the information tested. This includes examining all records and contracts that were applicable, testing for compliance with the prevailing rules and regulations of the county, as well as including other auditing procedures that we believe are necessary to complete this examination. We believe that the audit provides a reasonable basis for the audit findings and recommendations.

Major Findings

The Division of Information Technology (DOIT), the Police Department and Nassau Community College did not have complete, comprehensive, and up-to-date disaster-recovery plans. A county disaster Business Impact Analysis was performed in 1997, with participation from twelve county departments. Since 1997, the implementation of many new systems and applications has rendered this impact analysis out of date and in urgent need of revision.

DOIT's written disaster-recovery plan dates primarily from the period 1991-1993, again excluding many changes. With recent technological changes, the county's method of storing backup tapes appears outdated and is subject to risk due to the storage facility's close location to DOIT's Computer Center. It is of special concern that the separate recovery facility anticipated in DOIT's disaster recovery agreements can accommodate only limited staff. Departmental-end users--many performing essential services for county residents and employees--could not be accommodated.

Neither the Police Department nor Nassau Community College was able to furnish us with complete, comprehensive disaster recovery plans covering the vital systems they maintain.

Other Findings

Testing of disaster-recovery plans is not being done regularly. Specifically the AS/400 plan has not been tested since August 2000.

DOIT Response:

The Division of Information Technology has reviewed the above audit and its findings and recommendations. The Consulting firm, Denver Solutions Group has been retained to assist DOIT in conducting a review and update of the Business Impact Analysis last completed in November of 1997. We will keep your office apprised of the progress in completing this work as well as our work towards the issuance of a formal Disaster Recovery Plan for Information Technology Supported Systems.

Auditor's Comment:

We recommend that the Business Impact Analysis cover the county's entire system and not just the DOIT supported systems. It should identify the critical components, determine their inter-dependence and help in formulation of a comprehensive plan. We note DOIT has set a target date of December 31, 2002 for completion of the revised Disaster Recovery Plan.

Table of Contents

INTRODUCTION

FINDINGS AND RECOMMENDATIONS

Division of Information Technology

General

IBM Mainframe and AS/400 Systems

Table of Contents

FINDINGS AND RECOMMENDATIONS

Division of Information Technology

IBM Mainframe and AS/400 Systems (CONTINUED)

Network Systems and Mainframes (excluding IBM Mainframe and AS/400 Systems)

Storage of Backup Tapes

Nassau Community College

Table of Contents

FINDINGS AND RECOMMENDATIONS

Nassau County Police Department

APPENDIX

Introduction

Background

Disaster Preparedness

As the county's reliance on information technology appropriately increases, so does the danger that it will lose information collected by that technology unless it adopts a comprehensive disaster recovery plan. County officials are responsible for recognizing the probable causes of business interruptions and, to the extent possible, taking steps necessary to protect critical information technology operations. Even a short-term downtime of critical applications can cause a halting or delay in service delivery. Hardware redundancies and fault-tolerance operating systems are not necessarily adequate to address the risks posed by disasters such as fires and floods. Nassau must look at emerging technologies such as end-user computing, networks, electronic data interchange, and electronic data storage in formulating comprehensive disaster recovery plans.

Events that could result in county service interruptions include:

- Fire or flood
- Vandalism or sabotage (external/internal)
- Fraud
- Power failure
- Riot/civil disorder
- Human error
- Terrorist act
- Plane crash
- Computer hackers
- Earthquake
- Hurricane or tornado

An occurrence over the weekend of June 9th demonstrates the potential for serious impact due to one such event. The Department of Assessment's 6th floor Computer Room, located in the Nassau County Office Building at, 240 Old Country Road in Mineola, experienced extreme heat due to air conditioning failure over the weekend. Fortunately, the equipment only suffered some minor damage due to lack of air conditioning; however, if the incident had caused a prolonged period of disrepair, the absence of a proper disaster-recovery plan could have had the potential of a significant

The source for some of the information presented on this page is Auditing and Security, AS/400, NT, UNIX, Networks, and Disaster Recovery Plans, authored by Yusufali F. Musaji.

operational impact. As the room is unmanned over the weekends, staff was unaware of the situation until work resumed on Monday. Possibilities of housing the equipment in a location that is constantly manned should be looked into.

The county needs to identify its essential assets that need protection. One way to do this is to perform an impact study. Some essential assets (e.g., facilities, computer hardware and software) are tangible, easily identified and their value easily calculated. However, the value of data is more difficult to assess. When developing an inventory of essential assets requiring protection, consideration must be given to facilities, data, data-processing hardware, software, communications hardware, communications circuits and personnel. Designing a disaster recovery plan can be an expensive and labor-intensive task, which can take a year or more to complete.

Key Components of a Successful Disaster Recovery Plan

Successful DRPs are complete, current, and well documented. Specifically, the plan should describe the role of county officials, the recovery team's responsibilities, the distribution of completed plans, cost-effectiveness and operational feasibility, plan testing, recovery alternatives, critical operational procedures, and other emergency information that may be used in a long-term recovery environment. Specific statements regarding each of these areas will help to ensure that the DRP is comprehensive and complete enough to minimize the need for critical decision-making in a crisis situation.

As part of county officials' responsibility for ensuring the continuity of the county's services, they must ensure that adequate resources are available for planning, testing, and maintaining a comprehensive plan.

County Commitment and Funding

Disaster recovery requires additional resources and broader distribution of DRP responsibilities across the county. The county's DOIT is no longer the sole provider and sponsor for the county's DRP since the technology itself is no longer isolated in the controlled environment of major data centers. As with any business program, the DRP should be cost-effective and operationally feasible. County officials should identify the proper scope of

The source for some of the information presented on this page is Auditing and Security, AS/400, NT, UNIX, Networks, and Disaster Recovery Plans, authored by Yusufali F. Musaji.

the DRP based on the objectives of the plan, potential causes of service interruptions, possible economic consequences of disaster, potential legal liabilities, and organizational and non-organizational resources affected. It is possible to reduce costs by developing a plan that deals with only the worst-case scenario that can be modified for use in less serious disasters.

County officials should also determine the operational feasibility of the DRP. This step involves critically assessing the ability and desire of county staff to implement approved recovery procedures. The likelihood that key personnel will remain in a disaster situation to actually implement the plan should be addressed. Determining how recovery-team members and other employees will react to a disaster situation directly affects the structure and content of the DRP.

Recovery Teams

Disaster recovery teams should include county officials and senior staff, DOIT staff and end users qualified to help the county recover from interruption. Specific recovery teams may be organized to handle damage assessments, off-site facility administration, communications, hardware, software and general logistics. The DRP should include a notification section that contains the names, home addresses and telephone numbers of key personnel who need to be contacted in the event that a decision is made by county officials to declare a disaster. This notification section should also contain procedures and organizational charts identifying the appropriate sequence for contacting recovery team members following a disaster declaration.

How Should County Officials Define a Disaster?

Not every negative unplanned or spontaneous event or condition is a disaster, although it might be perceived as such. Some that cause only limited consequences are merely **interruptions**. An operational failure may fall into this category. **Emergencies** are disasters or significant interruptions, with potential for significant duration and impact on the county.

A DRP cannot depend on the participation of any particular employee or group of employees. The plan should describe key activities and critical decisions in sufficient detail so that any available staff member can perform required recovery tasks. A DRP should be as comprehensive as possible and

The source for some of the information presented on this page is Auditing and Security, AS/400, NT, UNIX, Networks, and Disaster Recovery Plans, authored by Yusufali F. Musaji.

should document pre-established criteria for making critical decisions in a crisis atmosphere. The plan should also provide details of required recovery actions and document retention policies. This information will become an important resource for the recovery process.

New York State Law: Article 2-B-State and Local Natural and Man-Made Disaster Preparedness

New York State law, §20, State and Local Natural and Man-Made Disaster Preparedness, Article 2-B, requires that local government and emergency service organizations have an essential role as the first line of defense in times of disaster. State policy requires that local chief executives take an active and personal role in the development and implementation of disaster preparedness programs and that they be vested with authority and responsibility in order to ensure the success of such programs. The state's policy also indicates that state and local plans, organizational arrangements, and response capabilities shall at all times be the most effective that current circumstances and existing resources allow.

§ 23 of Article 2-B addresses local disaster preparedness plans. Each county is authorized to prepare disaster preparedness plans. The purpose of such plans is to minimize the effect of disasters by identifying appropriate local measures to prevent disasters, developing mechanisms to coordinate the use of local resources and manpower for service during and after disasters and the delivery of services to aid citizens, and providing for recovery after disasters. Such plans shall include a specific plan for rapid and efficient communication and for the integration of local communication facilities during a disaster including the assignment of responsibilities and the establishment of communication priorities and liaison with municipal, private, state and federal communication facilities. The plan should also include criteria for establishing priorities with respect to the restoration of vital services.

Recommended Practices by GFOA

In 1999, the Government Finance Officers Association (GFOA) recommended the establishment of policies and procedures to minimize disruptions resulting from failures in computers or other advanced technologies following a disaster. At minimum, these policies and procedures should:

The source for some of the information presented on this page is Auditing and Security, AS/400, NT, UNIX, Networks, and Disaster Recovery Plans, authored by Yusufali F. Musaji.

- Formally assign disaster recovery coordinators for each agency or department to form a disaster recovery team.
- Require the creation and preservation of back-up data.
- Make provision for the alternative processing of data following a disaster.
- Provide detailed instructions for restoring disk files.
- Establish guidelines for the immediate aftermath of a disaster.

Objectives of Audit

Our overall objective was to ensure that the county's Division of Information Technology and key departments maintaining their own essential systems and applications have complete and effective disaster-recovery programs in place, which are kept current and tested on a regular basis. We attempted to determine that the disaster-recovery plans are adequate to insure resumption of computer systems in a timely manner during adverse circumstances. We reviewed contractual agreements to ensure that arrangements for an alternate site are in place in the event the county's computer facilities were rendered inoperable or destroyed in a disaster. We reviewed disaster recovery documentation and procedures for compliance with the practices recommended by the GFOA.

The Audit was performed during the first quarter of 2002.

Scope and Methodology

During the audit, we interviewed key staff responsible for the county's computer systems, and analyzed relevant disaster-recovery plans and other documentation. We reviewed the county's Business Impact Analysis (BIA), which gathered and analyzed data on the impact of a disaster on key functional areas. For the Division of Information Technology (DOIT), we reviewed disaster-recovery plans and procedures for major systems and applications--including the IBM mainframe, the AS/400, the SP2 mainframe, the Hewlett Packard 9000 mainframe, and network servers maintained by DOIT. We toured the DOIT Computer Center and the county's tape storage facility. We reviewed contractual agreements for a disaster-recovery facility and testing site outside of the county. At the Police Department, we reviewed Information Systems Bureau (ISB) disaster-recovery procedures and documentation for their department-wide computer network encompassing a variety of critical systems and applications. At

Nassau Community College's Management Information Systems Department (MIS), we reviewed disaster-recovery procedures and documentation for its IBM mainframe.

Discussion of Audit Results:

DOIT is in agreement with the audit's findings and will keep the Comptroller's Office apprised of their progress in the issuance of a formal Disaster Recovery Plan for Information Technology supported systems.

Findings and Recommendations

DIVISION OF INFORMATION TECHNOLOGY (DOIT)

Background:

DOIT provides 24-hour service, 365 days a year to county departments, agencies and divisions. It maintains computer-to-computer interfaces to statewide and national information systems. DOIT installs and customizes new business information systems and handles maintenance of existing systems. The DOIT system provides connectivity to the remote locations and data centers throughout Nassau County.

In 1997, twelve county departments participated in the preparation of a Business Impact Analysis (BIA) intended to gather and analyze data on key functional areas if a disaster were to occur to the DOIT service delivery system. The analysis established recovery priorities and tolerable outages in the event of a disaster. The number of critical functions that DOIT computer systems provide and county staff served by the county personal computer network, however, has grown considerably since 1997.

Audit Finding (1):

The BIA prepared in 1997 is outdated. Since 1997, material information-technology changes have taken place, including the implementation of NIFS (Nassau Integrated Financial System), the acquisition of the SP2 System (this computer mainframe provides services for the Board of Elections, the Traffic and Parking Violations Agency, and the Civil Service Commission), and the widespread networking of personal computers throughout the county. Close to 40 percent of departmental representatives participating in the 1997 BIA are no longer employed by the county. The BIA estimated the overall financial impact of an information-system outage (at day 6) at $400,000. This cost may have increased significantly.

Recommendation:

The county's BIA must be updated to reflect the current information technology systems and applications. Coordinators for each vital county agency or department should be formally assigned to form a team and to participate in the BIA. The BIA should:

- Identify critical systems, services, and operations.

- Identify and assess internal and external resources.
- Include a vulnerability analysis.
- List potential emergencies and estimate probability.
- Assess the potential human, property, and business impact of a disaster.
- Train the coordinators.

DOIT Response:

IT is in agreement with the recommendation. The previous Business Impact Analysis (BIA) was performed by IBM in 1997. The evolution of technology and applications as well as significant turnover in key personnel necessitates an update of this critical document. IT has contracted with Denver Research Solutions to conduct an in-depth review of the Business Impact of the loss of key IT support systems and to re-issue the report by 10/31/02. They will work with representatives of each vital agency and department in developing DR options and requirements.

Auditor’s Comment:

We agree with the corrective action taken by the DOIT.

IBM Mainframe and AS/400 Systems maintained by Division of Information Technology

Background:

DOIT is responsible for the maintenance of the county's IBM mainframe system. This system is necessary to conduct essential functions such as payroll, personnel, and accounting. It also maintains the AS/400, which is the County Clerk's primary mainframe computer system.

Audit Finding (2):

In 1991 the Department of General Service's Division of Data Processing, working with a consultant, Contingency Planning Research, developed a DRP. (The former Division of Data Processing is now part of the Department of Recreation, Parks, and Support Services and is known as the Division of Information Technology.) Much of the written plan, including the development of disaster scenarios, recovery strategies, establishment of command centers, and detail on the responsibilities of various disaster-recovery teams, dates to the period 1991-1993 and has not been updated.

Recommendation:

There have been many technological changes in the systems and applications utilized by the county since 1991. The county's departments and agencies increasingly rely on computer and other advanced technologies to conduct their operations. Additionally, there are many new recovery methods and processes that could be evaluated for inclusion in disaster-recovery procedures. The DRP itself called for the manual to be continually reviewed. DOIT must review and evaluate the plan for adequacy and completeness and update it as needed.

DOIT Response:

IT is in agreement with the recommendation. IT will undertake a review and re-writing of the Disaster Recovery Plan (DRP) for Information Technology. The Business Impact Analysis will be a key driver in the development of the updated Disaster Recovery Plan. This effort needs to be coordinated with the larger effort of preparing Disaster Recovery, Business Continuation and Crisis Management Plans for the county. IT will work with the Department of Emergency Operations or other lead agency to coordinate this effort. IT plans to complete the revised Disaster Recovery Plan for IT by 12/31/02.

Auditor's Comment:

We agree with the corrective action taken by the DOIT.

Audit Finding (3):

The DRP that was developed in 1991 called for a "Corporate Services Team," with representatives from key county departments such as Purchasing, Real Estate and Insurance, the County Executive, Public Works, and the Comptroller's Office. According to the plan, these team members would play significant roles in the event of a disaster, acting as liaisons for public relations, assisting in obtaining emergency supplies and equipment, supporting the recovery teams, and securing county buildings. Many of the original Corporate Services Team members have retired or left county service.

Recommendation:

Disaster-recovery precepts stress the need for a commitment from top officials to the importance of emergency management. County officials must be made aware of the importance of disaster recovery and their cooperation sought to making emergency management part of the county's "culture". The "Corporate Services Team" or its successor--which should include purchasing, financial, legal, human resources, engineering and maintenance, security, and community relations staff-- should receive timely updates on any changes in policies and procedures. County departmental staff should be trained in their responsibilities in the event of a disaster so that they can be ready to respond immediately.

DOIT Response:

While IT is in agreement with the recommendation, the required actions to fully implement it go far beyond the capability of the IT organization. This is a countywide initiative that needs to be coordinated by the county's Emergency Management organization. IT is committed to participating in this effort and to supply the Technology Disaster Recovery components as well as to participate in any training and drilling of the plans. The IT Steering Committee has been formed with representation from key operating departments and Chaired by the Commissioner of Accounts. This is currently the decision-making authority for changes in policy and procedures relating to IT support and governance. This Committee replaces the Corporate Services Team.

Auditor's Comment:

We concur.

Audit Finding (4):

DOIT uses RecoveryPAC (a software package) to control and update disaster- recovery resources, tasks and reports. RecoveryPAC is a relational data base product produced by Computer Security Consultants, Inc. In our review of the documentation stored in RecoveryPAC, the following exceptions were noted:

- Some data in RecoveryPAC were noted not to be current, or were lacking vital information. For example, information was missing or inaccurate for some records on:

  - Caller Lists ------ Incorrect phone number.
  - Equipment List -- Incomplete descriptive fields (i.e. size and weight of equipment, replacement value, and cost).
  - Software List ----- Missing revision numbers, release numbers and license numbers.
  - Critical Records -- Description, backup procedure, and restore procedure left blank.
  - Personnel File ---- Incorrect business phone number for an individual. "Business hours" was left blank.
  - Vendor List ------- Critical contact information was left blank. (Business hours and phone number.)

- **Use of RecoveryPAC is limited to one personal computer, which is located in the same building as the computer equipment it is required to assist in bringing back on line. It can be run only on this one personal computer. If a disaster encompassed the whole building (Old Court House), the RecoveryPAC software would be unusable.**

Recommendation:

DOIT must ensure that data on RecoveryPAC are updated whenever changes occur. Backup copies of RecoveryPAC should be kept off-site to ensure their availability in the event of a disaster.

DOIT Response:

IT is in agreement with the recommendation. IT will designate a second location, off-site from the Mineola complex, for the storage of critical recovery data and assure that both copies are updated quarterly.

Auditor's Comment:

We agree with the corrective action taken by the DOIT.

Audit Finding (5):

The county has two contracts with IBM. Under these contracts IBM provides a location at its Sterling Forest, New York facilities where DOIT staff participates in disaster-recovery testing. This facility will also provide a recovery center in the event of a disaster affecting the IBM mainframe and/or AS/400. The following concerns were noted in our review of the contractual agreements and discussion with DOIT staff that participate in disaster-recovery testing at Sterling Forest:

- In the event of a major disaster, the site would not fully accommodate DOIT staff and departmental end users. DOIT can bring the systems back up, with the terminals provided under the terms of both contracts. The equipment-configuration sheets of the business recovery services contracts for the IBM mainframe and the AS/400 do not provide for terminals for departmental end users. The end users of the system, such as the Comptroller's Payroll Section, the Treasurer's Office (tax payments), and Department of Assessment (tax records), as well as other vital departmental services, would not be able to function with such restrictions.

- Extended use of the recovery site is not addressed in detail in the contracts. Contract terms cover an initial recovery charge and a daily charge thereafter. A maximum period of usage is not addressed in the contracts. The contracts do not detail how long the county can use the facility, or establish a prioritization if many municipalities/organizations are affected by a wide spread disaster.

Recommendation:

Identify alternative sites, both "cold" and "hot", for possible long-term use. (A cold site provides the basics needed for recovery purposes, such as a vacant room with a raised floor, electrical outlets, air-conditioning equipment, chilled water, and perimeter security. A hot site is a site fully equipped and ready for use after a disaster.) The Sterling Forest business-recovery-services contracts, should be reviewed, and consideration given to contracting for a local cold site that would accommodate staff needed to keep all essential county departments functioning.

DOIT Response:

The review of hot and cold site alternatives will be included as part of the Business Impact Analysis discussed in Recommendation 1. The Sterling Forest contract with IBM will also be reviewed as part of this analysis. This review will only identify the requirements for recovery of IT systems and hardware, not for the off-site relocation of user department personnel. Those requirements should be identified in the countywide Business Continuation Plan prepared by Emergency Planning.

Auditor's Comment:

We concur.

Audit Finding (6):

Testing of disaster-recovery plans should take place regularly. The last recovery tests of the AS/400 were conducted in the summer of 2000. DOIT testing should occur at least on a semi-annual basis.

Employees were concerned that they had not been reimbursed on a timely basis for travel and other expenses incurred in traveling upstate. We were advised that recovery tests were almost postponed/halted due to this issue. This issue affected employee morale.

Recommendation:

DOIT officials must mandate and confirm that a regular testing schedule is followed for all critical applications and systems.

Because testing is a critical part of disaster recovery, necessary employees should be reimbursed appropriately to ensure their continuing participation.

DOIT Response:

IT is in agreement with the recommendation. Since the recommendation applies not only to systems and applications currently supported by IT, it is recommended that the IT Steering Committee oversee and receive periodic reports on the testing of critical systems in the county. The reimbursement of legitimate incremental expenses for employees who participate in the testing of these procedures will be provided.

Auditor's Comment:

We agree with the corrective action taken by the DOIT.

NETWORK SYSTEMS AND MAINFRAMES (EXCLUDING AS/400 AND IBM MAINFRAME) MAINTAINED BY DIVISION OF INFORMATION TECHNOLOGY

Audit Finding (7):

DOIT informed us of 45 network servers located in different locations throughout the county that are maintained by that department (see Appendix I). A SP2 Mainframe provides computer services for the Board of Elections, the Traffic and Parking Violations Agency, and the Civil Service Commission. A Hewlett Packard 9000 Main Frame computer system manages the Nassau County Geographic Information System (GIS). DOIT did not provide us with any comprehensive written disaster-recovery plan for these systems and applications.

Recommendation:

DOIT is responsible for recognizing the probable causes of interruptions and taking steps necessary to protect critical information-technology operations. DOIT must formulate a comprehensive written disaster-recovery plan and business-impact analysis and keep them current. An inventory of essential assets (facilities, hardware, and software, data, communications hardware and circuits, personnel) requiring protection should be developed and included in the plan.

DOIT must periodically test its computer disaster recovery-policies and take immediate action to remedy any deficiencies identified by that testing. It is essential that such testing encompass the restoration, as well as the processing of the data.

Currently, DOIT is using a program called RecoveryPAC to help maintain its disaster-recovery plan for the AS400 and IBM mainframe. RecoveryPAC stores disaster-recovery-plan data (i.e., personnel and equipment information). RecoveryPAC appears to be a comprehensive, detailed and user-friendly software package for disaster-recovery planning. The department may wish to consider the use of this program or a similar one in its disaster-recovery planning for the other systems and applications they maintain.

DOIT Response:

IT is in agreement with the recommendation. The scope of the Business Impact Analysis and Disaster Recovery Plan reviews discussed in recommendations 1 and 2 will be expanded to include all mid-range servers currently supported by IT. This will include all application, network, e-mail and web servers.

Auditor's Comment:

We agree with the corrective action taken by the DOIT.

Audit Finding (8):

DOIT did not confirm that the listing of operating systems and servers by department and location that we had compiled is complete and identifies all systems and servers within the county.

Recommendation:

DOIT should provide us with a list of all computerized systems, whether or not maintained by that department. It should ensure that all systems that may be essential to the county's disaster-recovery planning are reviewed on a required basis.

DOIT Response:

The Business Impact Analysis process will reach out to all departments and agencies to identify all applications and systems. As discussed in our response to recommendation 3, the IT Steering Committee has oversight responsibility for the entire county and would be the appropriate group to oversee the disaster-recovery planning for departments not currently supported by IT.

Auditor's Comment:

We concur.

STORAGE OF BACKUP TAPES

Audit Finding (9):

Regular backup tapes are made of key computer records, in accordance with predetermined schedules. These tapes are brought to a storage area located below Police Headquarters. Our tour of the facility and review of its use generated the following observations:

- The delivery of the tapes is subject to human error. For example: A tape could get physically damaged or misfiled.

- The storage facility is located on property abutting the DOIT Computer Center, located at the Old Court House, 1150 Franklin Avenue, Mineola. The close proximity could be a weakness, depending on the nature of a disaster.

- Because the storage facility is also a garage, temperature, climate, and ventilation could be a concern in maintaining the integrity/quality of the stored tapes. The below grade location of the facility could make it vulnerable to water damage in the event of a nearby fire or water-main problem.

Recommendation:

DOIT had researched alternative solutions and purchased a virtual tape system (a unmanned tape backup system), which has not yet been implemented. It is vital that alternative storage solutions be reviewed and one implemented as quickly as possible.

DOIT Response:

The process of off-site storage of daily backup tapes will be reviewed as part of the Disaster Recovery Plan review. Recommendations for how best to provide this vital function will be presented to the IT Steering Committee for approval and funding as necessary.

Auditor’s Comment:

We concur.

NASSAU COMMUNITY COLLEGE

Background:

The college's Management Information Systems Department (MIS) is responsible for the maintenance of the college's computer system and network applications. The system retains vital student, admission, registrar and bursar records. These records include students' prior-school records, grade, course, and class information, financial status records, financial aid information, immunization records, residency information/status, and student-billing information and records. Thirty-six staff members are assigned to MIS.

Audit Finding (10):

The college does not have a complete, written DRP for their mainframe computer system and network applications. In the event of a disaster, there is no backup-recovery-facility site designated. We were advised that MIS intends to implement a written plan in the near future. Although there is no written recovery plan, the MIS present daily operational procedures of restoring the system from backup tapes does provide some assurance that the system could be restored after a disaster.

Recommendation:

The college has established a disaster-recovery-implementation team, a MIS organization chart and an equipment inventory. Daily backups are performed and stored in a separate location. This is a starting point for the development and implementation of a comprehensive disaster-recovery plan. The plan should encompass project initiation and management, risk evaluation and control, a business impact analysis, the development of recovery strategies, and emergency response. It is essential that the college develop and implement the plan, develop awareness and training for staff and officials, test and evaluate the results, and keep the plan up to date.

DOIT Response:

IT is in agreement with the recommendation. While IT has not reviewed the work of the College, we would offer our services to review and comment on their plan. It may also be mutually advantageous to review any coordination opportunities that can be identified between the two DR plans.

Auditor's Comment:

The College should develop and implement a complete and comprehensive Disaster Recovery Plan by 12/31/02.

NASSAU COUNTY POLICE DEPARTMENT

Background:

The Police Department's Information Systems Bureau (Bureau) is responsible for coordinating the activities of the Police Department in developing and maintaining their computer-systems network and for the integration and implementation of the various technological programs and systems in use within the department as well as those contemplated for future implementation. 29 employees are currently assigned to the Bureau.

The Bureau provides statistics for state and federal agencies and for the Police Department administration. Its computer systems support critical applications and systems, including the Swift Justice Records Management System, the Computer Aided Dispatch System, the Mug Shot Photo System, and the Automated Fingerprint System. The Bureau is responsible for a department-wide computer network that supports more than 750 personal computers and 150 printers. This network connects 22 facilities over a Frame Relay Wide Area Network (WAN). There are 31 application and file servers on the department network; each utilizes an automatic tape backup. All servers and communications equipment are protected against power fluctuations and short-term blackouts through uninterruptible power supplies.

Audit Finding (11):

The Bureau does not have a complete and comprehensive disaster-recovery plan. We were provided with procedures in case of a crash of their server, emergency-callout procedures for Bureau personnel, and written detail on current disaster recovery-response-procedures; however, these items do not encompass a complete, comprehensive plan. In fact, in response to our request for their disaster-recovery procedures, the Bureau's commanding officer stated, "ISB is fully aware that the proper method to protect all of the data and equipment on the Police Department network would be to have a hot standby site capable of taking over the tasks in the event of an emergency. ISB does not have the facility, equipment and budget necessary to fully protect the systems in the event of an actual disaster."

Recommendation:

The Police Department should formulate a comprehensive written disaster-recovery plan and schedule a plan for its implementation. At a minimum, the department's policies and procedures should:

- Formally assign disaster recovery coordinators to form a disaster-recovery team.
- Require the creation and preservation of back-up data.
- Make provision for the alternative processing of data following a disaster.
- Provide detailed instructions for restoring disk files.
- Establish guidelines for the immediate aftermath of a disaster.
- Ensure that a copy of the disaster-recovery policies and procedures is kept off-site to ensure its availability in the event of a disaster.
- Provide for the periodic testing of the computer DRP and ensure that immediate action is taken to remedy deficiencies identified by that testing.

DOIT Response:

While IT fully endorses the need for a comprehensive disaster-recovery plan for the Police Department, a more cost effective solution may be the incorporation of these systems into a consolidated county-wide data center with it's associated disaster-recovery plan.

Auditor's Comment:

The Police Department should develop and implement a complete and comprehensive Disaster Recovery Plan by December 31, 2002. We agree that a more cost effective solution may be the incorporation of these systems into a consolidated countywide data center and the county should look into its feasibility.

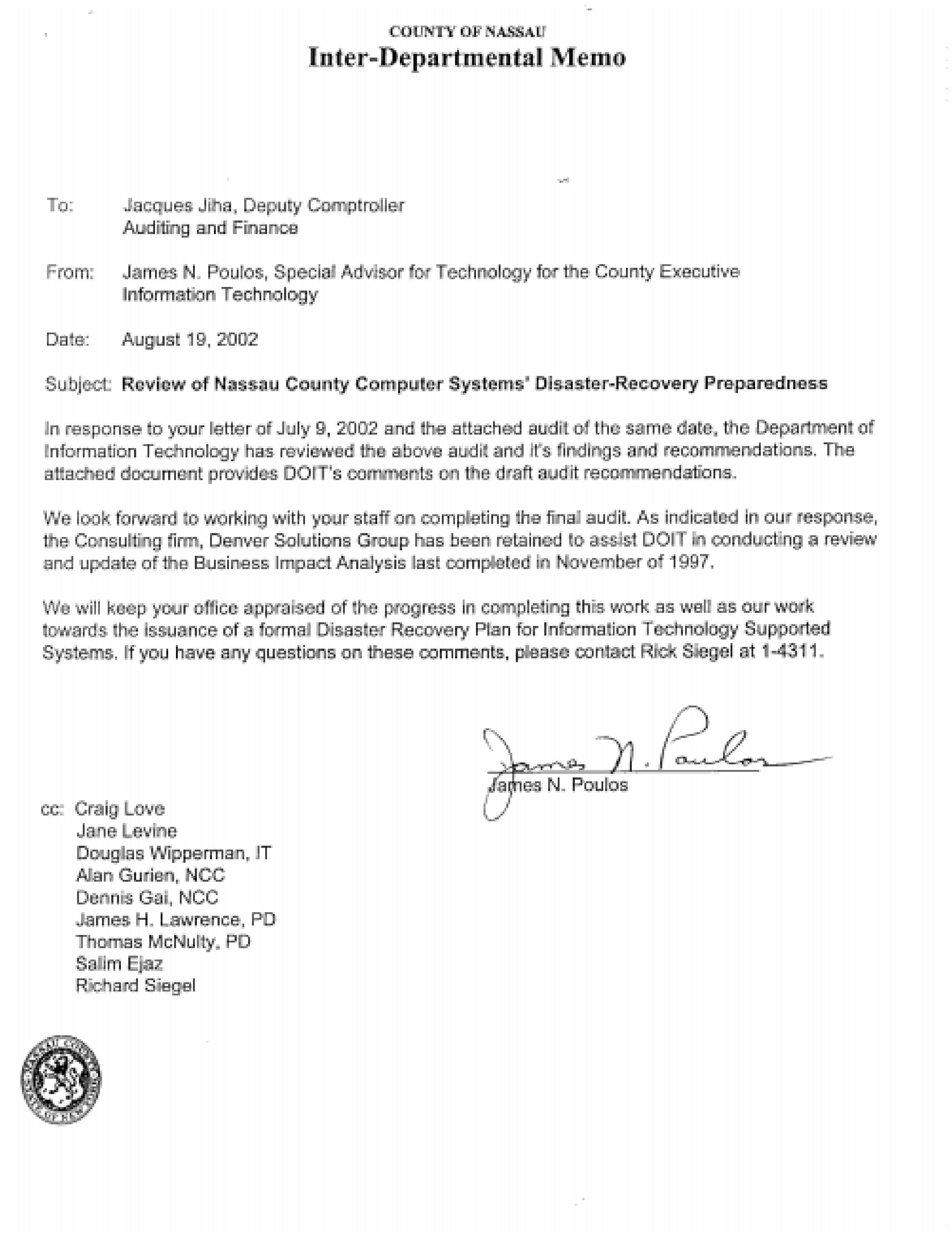
Appendix I

Network Servers Maintained by the Division of Information Technology

Operating System	Server Name	Department
Novell	FS_GS1	DDP, County Executive
Novell	FS_PWMN1	Department of Public Works
Novell	FS_CS	Civil Service
Novell	FS_240	Sheriffs, Treasurer, Comptrollers, County Clerk
Novell	FS_PARKS	Parks
Novell	FS_JAIL	Correction Center
Novell	FS_PLANNING	Planning
Novell	FS_CA	Consumer affairs
Novell	FS_PROBATION	Probation
Novell	FS_YB	Youth Board
Novell	FAX_SRV_GS1	DDP
Novell	FS_PWBP1	Department of Public Works
Novell	FS_PWCC1	Department of Public Works
Novell	FS_PWRV1	Department of Public Works
Novell	FS_PWSS1	Department of Public Works
Novell	FS_240BACKUP	DDP
Novell	1550_BACKUP	DDP
Novell	FS_PWMN2	Department of Public Works
Novell	FS_DDP	Department of Public Works
Novell	FS_NCFC	Fire Commission
Novell	FS_NCFTP1	DDP
Novell	FS_GISFTP	DDP
Novell	FEE	Probation
Novell	FS_SC	Senior Citizens
Windows NT4	FS_Mental Health	Mental Health
Windows NT4	Imaging	Department of Public Works
Windows NT4	Osprey	DDP
Windows NT4	Condor	DDP
Windows NT4	NTfaxsvr_ddp	DDP
Windows NT4	metaz1	DDP
Windows NT4	metaz2	DDP
Windows NT4	metaz3	DDP
Novell 4.11	dmi_gateway	DDP
Novell 4.11	Kestrel	DDP
Windows NT4	metadns1550	DDP
Solaris 2.7	Accipiter	DDP
Solaris 2.7	Caracara	DDP
Nokia 330 ipso	Harrier	DDP
Solaris 2.7	Buteo	DDP
Windows NT4	Erne	DDP
Solaris 2.8	nassweb01	DDP
Solaris 2.7	Nasseng	DDP
Windows NT4	Commmgt	DDP
Solaris 2.5	Netadm	DDP
AIX 4.3	devlp01	DDP

DDP = Division of Information Technology

Appendix II



COUNTY OF NASSAU

Inter-Departmental Memo

To: Jacques Jiha, Deputy Comptroller
Auditing and Finance

From: James N. Poulos, Special Advisor for Technology for the County Executive
Information Technology

Date: August 19, 2002

Subject: **Review of Nassau County Computer Systems' Disaster-Recovery Preparedness**

In response to your letter of July 9, 2002 and the attached audit of the same date, the Department of Information Technology has reviewed the above audit and it's findings and recommendations. The attached document provides DOIT's comments on the draft audit recommendations.

We look forward to working with your staff on completing the final audit. As indicated in our response, the Consulting firm, Denver Solutions Group has been retained to assist DOIT in conducting a review and update of the Business Impact Analysis last completed in November of 1997.

We will keep your office appraised of the progress in completing this work as well as our work towards the issuance of a formal Disaster Recovery Plan for Information Technology Supported Systems. If you have any questions on these comments, please contact Rick Siegel at 1-4311.

James N. Poulos

James N. Poulos

cc: Craig Love
Jane Levine
Douglas Wipperman, IT
Alan Gurien, NCC
Dennis Gai, NCC
James H. Lawrence, PD
Thomas McNulty, PD
Salim Ejaz
Richard Siegel

Information Technology Draft response comments to Audit of Nassau County Computer Systems' Disaster Recovery Preparedness. FA02-04 July 9, 2002

Recommendation 1 : "The County's BIA must be updated to reflect the current information technology systems and applications. Coordinators for each vital county agency or department should be formally assigned to form a team and to participate in the BIA."

IT Response: IT is in agreement with the recommendation. IBM performed the previous Business Impact Analysis (BIA) in 1997. The evolution of technology and applications as well as significant turnover in key personnel necessitates an update of this critical document. IT has contracted with Denver Research Solutions to conduct an in-depth review of the Business Impact of the loss of key IT support systems and to re-issue the report by 10/31/02. They will work with representatives of each vital agency and department in developing DR options and requirements.

Recommendation 2: "There have been many technological changes in the systems and applications utilized by the county since 1991. The county's departments and agencies increasingly rely on computer and other advanced technologies to conduct their operations. Additionally, there are many new recovery methods and processes that could be evaluated for inclusion in disaster recovery procedures. The DRP itself called for the manual to be continually reviewed. DOIT must review and evaluate the plan for adequacy and completeness and update it as needed."

IT Response: IT is in agreement with the recommendation. IT will undertake a review and re-writing of the Disaster Recovery Plan (DRP) for Information Technology. The Business Impact Analysis will be a key driver in the development of the updated Disaster Recovery Plan. This effort needs to be coordinated with the larger effort of preparing Disaster Recovery, Business Continuation and Crisis Management Plans for the County. IT will work with the Department of Emergency Operations or other lead agency to coordinate this effort. IT plans to complete the revised Disaster recovery Plan for IT by 12/31/02.

Recommendation 3: "Disaster Recovery precepts stress the need for a commitment from top officials to the importance of emergency management. County officials must be aware of the importance of disaster recovery and their cooperation sought to making emergency management part of the county's "culture". The "Corporate Services Team" or it's successor which should include purchasing, financial, legal, human resources, engineering and maintenance, security, and community relations staff should receive timely updates on any changes in policy and procedures. County departmental staff should be trained in their responsibilities in the event of a disaster so that they can be ready to respond immediately."

IT Response: While IT is in agreement with the recommendation, the required actions to fully implement it go far beyond the capability of the IT organization. This is a countywide initiative that needs to be coordinated by the county's Emergency Management organization. IT is committed to participating in this effort and to supply the Technology Disaster Recovery components as well as to participate in any training and drilling of the plans. The IT Steering Committee has been formed with representation from key operating departments and Chaired by the Commissioner of Accounts. This is currently the decision-making authority for changes in policy and procedures relating to IT support and governance. This Committee replaces the Corporate Services Team.

Recommendation 4: "DOIT must ensure that data on RecoveryPAC are updated whenever changes occur. Backup copies of ReoveryPAC should be kept off-site to ensure their availability in the event of a disaster."

IT Response: IT is in agreement with the recommendation. IT will designate a second location, off-site from the Mineola complex, for the storage of critical recovery data and assure that both copies are updated quarterly.

Recommendation 5: "Identify alternative sites, both "cold" and 'hot", for possible long-term use. (A cold site provides the basics needed for recovery purposes, such as a vacant room with a raised floor, electrical outlets air conditioning equipment, chilled water, and permanent security. A hot site is a site fully equipped and ready for use after a disaster.) The Sterling Forest business-recovery-services contract should be reviewed, and consideration given to contracting for a local cold site that would accommodate staff needed to keep all essential county departments functioning."

IT Response: The review of hot and cold site alternatives will be included as part of the Business Impact Analysis discussed in Recommendation 1. The Sterling Forest contract with IBM will also be reviewed as part of this analysis. This review will only identify the requirements for recovery of IT systems and hardware, not for the off-site relocation of user department personnel. Those requirements should be identified in the countywide Business Continuation Plan prepared by Emergency Planning.

Recommendation 6: "DOIT officials must mandate and confirm that a regular testing schedule is followed for all critical applications and systems. Because testing is a critical part of disaster recovery, necessary employees should be reimbursed appropriately to ensure their continuing participation."

IT Response: IT is in agreement with the recommendation. Since the recommendation applies not only to systems and applications currently supported by IT, it is recommended that the IT Steering

Committee oversee and receive periodic reports on the testing of critical systems in the county. The reimbursement of legitimate incremental expenses for employees who participate in the testing of these procedures will be provided.

Recommendation 7: "Currently DOIT is using a program called RecoveryPAC to help maintain their disaster recovery plan for the AS-400 and IBM mainframe. RecoveryPAC stores disaster-recovery-plan data (i.e., personnel and equipment information). RecoveryPAC appears to be a comprehensive, detailed and user-friendly software package for disaster-recovery planning. The Department may wish to consider the use of this program or a similar one in their disaster-recovery-planning for the other systems and applications they maintain."

IT Response: IT is in agreement with the recommendation. The scope of the Business Impact Analysis and Disaster Recovery Plan reviews discussed in recommendations 1 and 2 will be expanded to include all mid range servers currently supported by IT. This will include all application, network, email and web servers.

Recommendation 8: "DOIT should provide us with a list of all computerized systems, whether or not maintained by that department. It should ensure that all systems that may be essential to the county's disaster-recovery planning are reviewed on a required basis."

IT Response: The Business Impact Analysis process will reach out to all departments and agencies to identify all applications and systems. As discussed in our response to recommendation 3, the IT Steering Committee has oversight responsibility for the entire county and would be the appropriate group to oversee the disaster-recovery planning for departments not currently supported by IT.

Recommendation 9: "DOIT had researched alternative solutions and purchased a virtual tape system (a unmanned tape backup system), which has not yet been implemented. It is vital that alternative storage solutions be reviewed and one implemented as quickly as possible."

IT Response: The process of off-site storage of daily backup tapes will be reviewed as part of the Disaster Recover Plan review. Recommendations for how best to provide this vital function will be presented to the IT Steering Committee for approval and funding as necessary.

Recommendation 10: "The College has established a disaster-recovery-implementation team, a MIS organization chart, and an equipment inventory. Daily backups are performed and stored in a separate location. This is a starting point for the development and implementation of a comprehensive disaster-recovery plan. The plan should encompass project initiation and management, risk evaluation and control, a business impact analysis, the development of recovery strategies, and emergency response. It is essential that the College develop and implement the plan, develop awareness and training for staff and officials, test and evaluate the results, and keep the plan up to date."

IT Response: IT is in agreement with the recommendation. While IT has not reviewed the work of the College, we would offer our services to review and comment on their plan. It may also be mutually advantageous to review any coordination opportunities that can be identified between the two DR plans.

Recommendation 11: "The Police Department should formulate a comprehensive written disaster-recovery plan and schedule a plan for implementation."

IT Response: While IT fully endorses the need for a comprehensive disaster-recovery plan for the Police department, a more cost effective solution may be the incorporation of these systems into a consolidated county-wide data center with it's associated disaster-recovery plan.